The second problem set

Due 10/22/14.

Recall that for any prime p and any positive integer n, $v_p(n)$ is the power of p in the prime factorization of n.

And so $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ and $v_p(mn) = v_p(m) + v_p(n)$.

1. Prove that for any positive integers m and n we have

(a) $v_p(\gcd(m,n)) = \min\{v_p(m), v_p(n)\}$,

(b) $v_p(\operatorname{lcm}(m,n)) = \max\{v_p(m), v_p(n)\}$, where $\operatorname{lcm}(m,n)$ is the least common multiple of m and n.

(c) $\gcd(m,n) \cdot \operatorname{lcm}(m,n) = mn$.

[Hint: Use what we proved in class:

$$d \mid n \iff \forall p \in \mathcal{P},\ v_p(d) \le v_p(n).$$

For part (c) use $\min\{x,y\} + \max\{x,y\} = x+y$.]

2. Let m and n be positive integers. Prove that

$$d \mid m \text{ and } d \mid n \iff d \mid \gcd(m,n).$$

3. Let n be a positive integer. Prove that n is a perfect square, i.e. $n = a^2$ for some integer a, if and only if $d(n)$ is odd, where $d(n)$ is the number of positive divisors of n.

4. Prove that $\sqrt{2}$ is irrational.

[Hint: Suppose to the contrary that $\sqrt{2} = \frac{m}{n}$.

$\Rightarrow 2n^2 = m^2$. Consider $v_2(2n^2) = v_2(m^2)$.]

5. Suppose n is a positive integer. Suppose

$$p \mid n \text{ and } p \text{ is prime} \Rightarrow p > n^{1/k}$$

where $k \in \mathbb{Z}^{\geq 2}$.

Prove that n is a product of at most $k-1$ primes. (NOT necessarily distinct.)

[Hint: Suppose to the contrary that

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_\ell$$

where p_i's are prime and $\ell \geq k$.]

6. Prove that there are infinitely many primes of the form $4k-1$.

[Hint: Suppose to the contrary that there are only finitely many of such primes: $p_1, p_2, \dots, p_n$. Consider $N = 4p_1p_2\cdots p_n - 1$. And notice that $4 \mid x-1$ and $4 \mid y-1 \Rightarrow 4 \mid xy-1$.]

7. Let $(G, *)$ be a group. For $g \in G$, let

$$\ell_g : G \to G, \quad \ell_g(g') := g * g'.$$

(a) Prove that $\ell_{g_1} \circ \ell_{g_2} = \ell_{g_1 * g_2}$; and

(b) $\ell_e = id_G$ where e is the identity element of G, and $id_G : G \to G$ is the identity function.

(c) ℓ_g is invertible and $\ell_g^{-1} = \ell_{g^{-1}}$.

(d) If $\ell_g(g') = g'$ for some $g' \in G$, then $g = e$.